**Hastings Law Journal**

Volume 53 | Issue 2 Article 5

1-2002

# Satellite Tracking and the Right to Privacy

Aaron Renenger

# Satellite Tracking and the Right to Privacy

*by*
AARON RENENGER*

> What are the implications for individual privacy in a world where millions of people are driving Internet-enabled cars that have their movements monitored at all times?
>
> —IBM Chairman and CEO Lou Gerstner

## Introduction

In the span of just a few decades the information age has altered the way we communicate and brought the world closer together. However, the new technologies of the age have brought with them an all-too-familiar challenge—how to ensure personal privacy. In their famous 19th-century law review article on privacy, Samuel Warren and Louis Brandeis wrote words which ring equally true today:

> The intensity and complexity of life . . . have rendered necessary some retreat from the world . . . so that solitude and privacy have become more important to the individual; but modern enterprise and invention have, through invasions upon [a man's] privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury.[1]

Fueled by news accounts of potential privacy abuses on the Internet, privacy has become one of the leading concerns of American consumers.[2] One new technology that greatly concerns privacy advocates is the Global Positioning System ("GPS"), a satellite-based navigation system that can provide a consumer, and possibly third parties, with a precise reading of the person's location. Privacy advocates are wary of GPS because, as explained by

* J.D. Candidate, University of California, Hastings College of the Law 2002; B.A. California State University, Sacramento.

1. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193, 196 (1890).

2. A. Michael Froomkin, *The Death of Privacy*, 52 Stan. L. Rev. 1461, 1467 n. 16 (2000).

Laurence Tribe, "[p]art of human dignity is the ability to hide. Even in the context of someone you trust to act in your own interest, there are a great many things with respect to your location over which you want to retain authority."[3]

This note assumes that in order for GPS technology to truly proliferate, consumers must be assured of the privacy of their location information—a view that is shared by privacy advocates as well as the telecommunications industry.[4] Therefore, Congress, federal regulatory agencies, state legislatures, and the courts must act now to protect consumer privacy related to positioning technology.

Part I of this note explains GPS technology and discusses how some of its uses have prompted concern among privacy advocates. Part II analyzes privacy law as it exists now and discusses its applicability to the GPS context. Finally, part III examines tort proposals created to prevent the unauthorized release of location information.

## I. GPS Technology and Its Uses

GPS is based on a network of at least 24 satellites that continuously send out radio signals transmitting their locations.[5] A GPS receiver back on Earth can then triangulate its three-dimensional position using the information received from at least four of the satellites.[6] The system is accurate anywhere on Earth to within 100 feet.[7] Using a technique called differential GPS, users can obtain accuracies of several feet.[8]

Originally developed by the Department of Defense as a means of navigating submarines and guiding missiles, GPS is today used in numerous creative commercial applications, creating an expected global market of $19 billion for GPS equipment and location services in 2001.[9]

---

3. M.J. Zuckerman, *Wireless, With Strings Attached. A Cellphone Can Make You Stand Out, to Rescuers and Marketers Alike*, USA TODAY, Feb. 7, 2001, at 1D.

4. Petition of the Cellular Telecommunications Industry Association for a Rulemaking to Establish Fair Location Information Practices at 4-5, In the matter of Petition for Rulemaking (Nov. 22, 2000).

5. Fact Sheet, United States Air Force, NAVSTAR Global Positioning System (October 1999) *available at* http://www.af.mil/news/factsheets/NAVSTAR_Global_Positioning_Sy.html.

6. *See id.*

7. *Id.* The system now attains accuracy of within forty-eight to sixty feet after the federal government in 2000 turned off a feature that intentionally degraded the civilian signal. Kevin Washington, *Locator System Draws Bead on Better Accuracy*, BALT. SUN, May 8, 2000, at 1C.

8. David H. Freedman, *Flying Made Easy*, TECH. REV., Mar. 1, 2001, at 59.

9. *Wireless World Will Drive GPS Applications, According to New Allied Business Intelligence Study*, BUSINESS WIRE, Dec. 13, 2000. Further, by 2005, the GPS market is

Many municipalities and businesses now use the system for vehicle fleet management,[10] and millions of personal cars will soon have GPS navigation available to the driver.[11] GPS is even used for such exotic functions as tracking migration patterns of animals.[12]

Perhaps no application has resulted in as great a proliferation of GPS technology as the pending Federal Communications Commission ("FCC") requirement for telecommunications companies to integrate positioning service into cellular-phone handsets.[13] Originally, cell-phone companies were to have begun selling location-capable handsets no later than October 1, 2001.[14] Mobile-service providers did not meet the deadline, however, because they claimed that "the technology to provide the service was still being built."[15] Consequently, the FCC is now requiring companies to file quarterly reports of their progress towards implementing the system, with a goal that 95% of all handsets be in compliance by 2005.[16]

The requirement is part of the FCC's Enhanced 911 ("E-911") regulations which "are intended to improve the reliability of wireless 911 services, by requiring wireless carriers to provide to emergency dispatchers information on the location from which a wireless call is being made."[17]

Telecommunications companies may provide the requisite positioning information through either network-based technology (e.g., triangulation utilizing the existing cellular tower infrastructure)

---

expected to reach $60 billion.

10. Pat Thompson, *Postal Service to Monitor Carriers with Satellite Tracking System*, FORT WORTH STAR TELEGRAM, May 16, 1996, at 4.

11. One such personal-vehicle system, OnStar, is projected to be available in over four-million cars by 2003. Press Release, OnStar, GM's OnStar Subsidiary Brings Location-based, Real-Time Traffic and Road Condition Information Into the Vehicle (Nov. 13, 2000) (on file with author).

12. Jeffrey P. Cohn, *Tracking Wildlife: High-tech Devices Help Biologists Trace the Movements of Animals Through Sky and Sea*, BIOSCIENCE, January, 1999, at 13.

13. FCC 911 Service Rule, 47 C.F.R. § 20.18 (1999); *see also* Simon Romero, *Location Devices' Use Rises, Prompting Privacy Concerns*, N.Y. TIMES, March 4, 2001, at 1.

14. 47 C.F.R. § 20.18.

15. Suzanne King and David Hayes, *Deadline Extended for 911 Technology; Location Capability Must be in Place by 2005, FCC says*, THE KANSAS CITY STAR, Oct. 9, 2001, at D10.

16. FCC Commissioner Kathleen Abernathy, Separate Statement *In re*: Revision of the Commission's Rules To Ensure Compatibility with Enhanced 911 Emergency Calling Systems (Oct. 2, 2001), *available at* http://www.fcc.gov/Speeches/Abernathy/Statements/2001/stkqa106.html.

17. Press Release, Federal Communications Commission, FCC Adjusts Its Rules to Facilitate the Development of Nationwide Enhanced Wireless 911 Systems (Sept. 8, 2000), *available at* http://www.fcc.gov/e911/.

or through handset-based technology like GPS.[18] Network-based technologies must be able to locate callers to within 100 meters 67% of the time, while handset-based technologies must be able to locate callers to within 50 meters 67% of the time.[19] Verizon Wireless and Western Wireless have chosen to develop network-based solutions, while Sprint PCS, Alltel, and Nextel are developing GPS-based systems.[20]

The Cellular Telecommunications and Internet Association ("CTIA")[21] and others insist that new consumer benefits will abound because of the availability of positioning information.[22] Through network and handset-based technologies, a subscriber to a location service can access driving directions, local news or weather, traffic delay updates, and even concierge services to make dinner reservations.[23] Location-sensitive content, advertising, and personalization services are already being deployed by companies like Airflash, ViAir, and AdForce.[24]

But it is precisely the technology that enables these consumer benefits that has privacy advocates concerned.[25] Many fear that cell-phone companies could use the location information to constantly monitor the location of their customers.[26] Privacy advocates have referred to the technology as "digital dog tags"[27] and warned that the information could be sold to aggressive advertisers or accessed by criminals.[28]

Location information could conceivably be cross-referenced with existing database information regarding a consumer's habits. Voluminous information regarding consumer habits can already be compiled via the Internet.[29] "On the Internet, every Web site we visit,

18. 47 C.F.R. § 20.18.

19. *Id.*

20. Romero, *supra* note 13, at 25.

21. The organization changed its name in 2001 from the Cellular Telecommunications Industry Association. The acronym CTIA remains unchanged.

22. Petition of the Cellular Telecommunications Industry Association for a Rulemaking to Establish Fair Location Information Practices at 4-5, In the matter of Petition for Rulemaking (Nov. 22, 2000).

23. *Id.*

24. *Id.*

25. Romero, *supra* note 13.

26. *See* Hiawatha Bray, *Something to Watch Over You; Your Cell Phone Is a Homing Beacon, and Soon It Will Be Tracking Your Every Move*, THE BOSTON GLOBE, Jan. 22, 2001, at C1.

27. Keith Perine, *Talking About Wireless Privacy*, THE INDUSTRY STANDARD, Dec. 25, 2000.

28. Jube Shiver Jr., *Prying-Eye Phone Technology Raising Privacy Concerns*, L.A. TIMES, Dec. 12, 2000, at C1.

29. JEFFREY ROSEN, THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA 159-95 (Random House 2000).

every store we browse in, every magazine we skim, and the amount of time we spend skimming it, create electronic footprints that increasingly can be traced back to us, revealing detailed patterns about our tastes, preferences and intimate thoughts."[30] Privacy advocates fear that advertisers will combine this consumer preference data with location information to unleash a barrage of personalized ads onto a person's mobile phone.[31] Imagine walking through a mall anywhere in the nation as your cell phone rings, displaying the latest sales prices in the store by which you are walking.

Other parties with an interest in knowing your whereabouts could theoretically also use location information. As explained by James Dempsey of the Center for Democracy and Technology, "what if your insurer finds out you're into rock climbing or late-night carousing in the red-light district? What if your employer knows you're being treated for AIDS at a local clinic? The potential is there for inferences to be drawn about you based on knowledge of your whereabouts."[32] In short, privacy advocates are concerned that cell-phone companies will release location information to third parties—whether the third party is a marketer, a law enforcement agency, an employer, or a criminal.

The E-911 requirement is not the only GPS application that concerns privacy advocates. For example, several companies are offering GPS-based devices small enough to be worn on a tennis shoe or around the wrist.[33] Though designed as a means for parents to keep tabs on their children,[34] some privacy analysts are concerned that the same devices will be used by stalkers and private detectives to accurately obtain knowledge of a person's whereabouts.[35]

General Motors is integrating "black box" technology into its cars.[36] Coupled with GPS, the boxes could record exactly where the

30. *Id.* at 7.

31. Shiver, *supra* note 28 (explaining that "cell phone companies and marketers will know not only who [users] are, but also where they are within a few feet and perhaps what consumers are buying while they are in a store"); *see, e.g.*, Anne Colden, *Privacy Concerns Expected to Grow*, THE DENVER POST, Jan. 1, 2001, at E-01 (discussing the Privacy Foundation's concerns about profiling of individuals in order to target personalized wireless ads).

32. Romero, *supra* note 13, at 25.

33. Ward, *supra* note 33, at 1; *see, e.g.*, Steve Shoup, *Baca Fears Tracking System May Invite Abuse*, ALBUQUERQUE J., Aug. 22, 2000, at B2 (discussing proposal by Albuquerque mayor Jim Baca to criminalize tracking an individual without consent).

34. Ward, *supra* note 33, at 1 (explaining that a missing child can be pinpointed in thirty seconds).

35. *Id.*; *see also* Colden, *supra* note 31.

36. Bob Van Voris, *Black Box Car Idea Opens Can of Worms*, NAT'L L. J., June 14, 1999, at A1.

car has been and whether the driver was breaking any driving laws.[37] This formerly hypothetical scenario became reality in the summer of 2001 when an Acme Rent-A-Car franchise in New Haven, Connecticut began fining consumers for speeding in their rented vehicles.[38] The company's vehicles were equipped with GPS boxes that recorded the location and speed of the vehicles.[39] The policy became a national news story when one consumer was fined $450 for three separate speeding incidents.[40] The consumer has since brought suit in Connecticut state court and filed a complaint with the Connecticut Department of Consumer Affairs.

Meanwhile, the Federal Highway Administration, along with the states of California, Minnesota, Iowa, Kansas, Michigan, Texas, Washington, and Wisconsin are conducting a joint research project about the feasibility of using GPS-based systems to collect information from vehicles for road use charges.[41] Insurance companies are experimenting with a similar system designed to charge for insurance based on miles driven.[42] Privacy advocates fear these records will be subpoenaed by law enforcement.[43]

On the criminal front, the use of GPS has already raised a Fourth Amendment privacy claim in at least one circuit court case.[44] In *United States v. McIver*, the Ninth Circuit Court of Appeals upheld the warrantless placement of a GPS-based tracking device by law enforcement on the undercarriage of a suspect's vehicle.[45] The court held that the placement of the device was neither a search nor a seizure.[46]

The court held it was not a search because the undercarriage is part of the exterior of the vehicle,[47] and according to the Supreme Court in *New York v. Class*,[48] there is no reasonable expectation of privacy in the exterior of a vehicle. The court held that no seizure occurred because the device represented only a technical trespass on

37. *Id.*

38. Colleen Van Tassell, *GPS: Gotta Pay for Speeding*, NEW HAVEN ADVOCATE, June 14, 2001.

39. *Id.*

40. *Id.*

41. *States Eye GPS for Road Tax Collection*, GLOBAL POSITIONING & NAVIGATION NEWS, Nov. 29, 2000. If adopted, the system may ultimately be used in lieu of fuel taxes by charging taxpayers per mile driven.

42. Anne Eisenberg, *Buy Car Insurance By the Mile*, DAYTON DAILY NEWS, Apr. 24, 2000, at 1.

43. *Id.*

44. United States v. McIver, 186 F.3d 1119, 1126-27 (9th Cir. 1999).

45. *Id.*

46. *Id.*

47. *Id.*

48. 475 U.S. 106 (1986).

the space occupied by the beeper, and the beeper in no way deprived the defendant of dominion and control over his vehicle.[49]

## II. The Current State Of Privacy Law And It's Applicability To GPS-Based Tracking

Privacy has been defined as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[50] The "information" referred to in this definition could include any personal information that a person wishes to keep to herself, including that person's exact location at any given time.

Privacy, of course, has been most widely implicated in criminal cases by the Fourth and Fifth Amendments to the United States Constitution.[51] It has also been famously implicated by the Supreme Court in cases like *Griswold v. Connecticut*.[52] These cases, however, involve the protection of personal privacy from invasion by the federal or state governments. "Whereas the Constitution insulates individuals from governmental intrusion into their private lives, it does not dictate rights between private citizens."[53]

While the privacy of individuals to be free from governmental intrusion is certainly implicated by the debate over GPS, criminal procedure and the Supreme Court's Fourth Amendment jurisprudence will most likely shape the contours of that particular debate.[54] It is beyond the scope of this note to analyze the constitutionality of law enforcement's use of GPS.[55] Rather, this paper focuses on the rights of individuals as against private parties.

### A. The Invasion of Privacy Torts

A privacy tort has been recognized in the United States at least since the publication of the famous 1890 Warren and Brandeis article on the subject.[56] In that article, the authors explained that "[t]he

49. *McIver*, 186 F.3d at 1127.

50. ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (Ass'n of the Bar of the City of New York 1967).

51. U.S. CONST. amend. IV, V.

52. 381 U.S. 479 (1965).

53. Diane L. Zimmerman, *Requiem for a Heavyweight: A Farewell to Warren and Brandeis's Privacy Tort*, 68 CORNELL L. REV. 291, 298 (1983).

54. *See, e.g.*, *McIver*, 186 F.3d at 1126-27.

55. For a discussion of the law enforcement issues, the reader should consult *McIver*, *id.*, and *United States v. Karo*, 458 U.S. 705 (1984) (discussing the analogous area of tracking a suspect's vehicle with a non-GPS-based "beeper").

56. Warren and Brandeis, *supra* note 1; Sidis v. F-R Pub. Corp., 113 F.2d 806, 808 (2d Cir. 1940) (explaining that "[a]ll comment upon the right of privacy must stem from the famous article by Warren and Brandeis on The Right of Privacy . . ."); *see also* Solveig

common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others."[57]

In "Warren and Brandeis's formulation, the 'right to privacy' referred to a right not to have information about one's personal life exposed to the general public by the press."[58] Following publication of the article, numerous state courts acted to incorporate the Warren-Brandeis theory as well as several other related privacy torts.[59] There are now four privacy torts recognized by the Restatement (Second) of Torts: the false light tort, the tort of intrusion upon seclusion, the misappropriation tort, and the tort of publicity of a person's private life.[60]

None of these torts applies easily to the GPS context. Any invasion of privacy tort possibly raises an issue regarding the First Amendment rights of the party violating the privacy. This issue will be discussed later in the context of *U.S. West, Inc. v. Federal Communications Commission*.[61]

A GPS-based claim arising under the false-light tort is unlikely to survive a summary judgment motion because truth is a defense to this claim.[62] The potential privacy invasion concerning the use of GPS, on the other hand, is not based on falsity, but on dissemination of truthful information that a consumer would prefer to keep private. For example, the fact that a woman may have recently visited an abortion clinic may not be untrue, but is nevertheless a matter she may prefer to keep quiet.

The misappropriation tort, meanwhile, is limited to the use of another's name or image for commercial gain.[63] It has perhaps most widely been applied in protecting celebrities' right of publicity.[64] Any use of GPS information, on the other hand, involves not a person's name or image, but knowledge of that person's precise whereabouts.

The public disclosure of private facts tort is conceivably available to a GPS plaintiff. The tort arises when a party publicizes

Singleton, *Privacy Versus the First Amendment: A Skeptical Approach*, 11 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 97, 109 (2000).

57. Warren & Brandeis, *supra* note 1, at 198.

58. Zimmerman, *supra* note 53, at 291, 295.

59. Singleton, *supra* note 56, at 109.

60. RESTATEMENT (SECOND) OF TORTS § 652A (1977).

61. 182 F.3d 1224 (10th Cir. 1999).

62. RESTATEMENT (SECOND) OF TORTS § 652E; Singleton, *supra* note 56, at 110.

63. Abdul-Jabbar v. General Motors Corp., 85 F.3d 407, 413-14 (9th Cir. 1996) (listing "appropriation of a plaintiff's name or likeness" as a requisite element); RESTATEMENT (SECOND) OF TORTS § 652C.

64. *See, e.g.*, Carson v. Here's Johnny Portable Toilets, Inc., 698 F.2d 831, 837 (6th Cir. 1983) (finding that television personality Johnny Carson's right of publicity was violated where the defendant gained commercially through its use of the phrase "Here's Johnny").

information of a kind that would be highly offensive to a reasonable person and the information is not of legitimate concern to the public.[65]

But application of the tort has been strictly limited. For example, if an event takes place in a public place, the tort is unavailable.[66] After all, when a person travels over the public streets, "he voluntarily convey[s] to anyone who want[s] to look the fact that he [is] traveling over particular roads in a particular direction, the fact of whatever stops he [makes], and the fact of his final destination."[67] Thus if a lender gleans from a loan applicant's cell phone records that the applicant has spent an unusual amount of time at the horse races lately, the applicant would probably not have a cause of action under the public disclosure of private facts tort as it has been applied by the courts.[68]

Recovery is also not available if the fact the person desires to keep private is not widely circulated by a defendant, but only released to a select group of people.[69] Thus, if an employer decides not to hire a job applicant because, through exploitation of cell-phone data, the employer discovers that the applicant makes weekly visits to an AIDS clinic,[70] there would be no cause of action against the party who released the location data for publication of private information.

Finally, if the embarrassing information is about a public figure, the matter may usually be reported as a matter of public record.[71] The California Supreme Court explained that "[t]hose who seek elected public positions realize that in so doing they subject themselves, and those closely related to them, to a searching beam of

65. RESTATEMENT (SECOND) OF TORTS § 652D.

66. *Id.* at cmt. b.

67. United States v. Knotts, 460 U.S. 276, 281-82 (1982) (holding that police did not commit a Fourth Amendment violation by using a beeper to track the location of a suspect's automobile).

68. The fact that a person is visiting a public establishment does not always defeat an invasion of privacy tort. *See* Doe v. Mills, 536 N.W.2d 824, 832 (Mich. App. 1995) (holding that the fact that women could be seen entering and exiting a public in vitro fertilization clinic was not a defense to an invasion of privacy tort against a group of abortion protestors who held large signs naming the plaintiffs as baby killers). Here, the court felt that the information disclosed took place within the private confines of a clinic. *Id.* It is doubtful whether this exception could be applied in the context of a visit to the racehorses, since the confines of a racetrack are still presumably a public place.

69. RESTATEMENT (SECOND) OF TORTS § 652D cmt. a.

70. The facts of this hypothetical differ only slightly from those of *McNemar v. Disney Stores, Inc.*, 4 Am. Disabilities Cas. (BNA) 897 (1995) (finding that there was no invasion of privacy "to communicate a fact concerning the plaintiff's private life to a single person or even to a small group of persons" where one Disney employee revealed to plaintiff's boss that plaintiff was HIV-positive).

71. RESTATEMENT (SECOND) OF TORTS § 652D cmt. e.

public interest and attention."[72] Thus, if a newspaper reporter obtains a political candidate's cell-phone records and discovers that the candidate has a propensity to engage in gambling, the candidate would not likely have a cause of action.

Of all the privacy torts, the intrusion upon seclusion tort could most easily be applied in the GPS context. This tort is available against a person who intrudes on the solitude or seclusion of another if the intrusion would be highly offensive to a reasonable person.[73] This intrusion need not be physical, but would include any intrusion, such as eavesdropping, onto an individual's private concerns.[74] Thus, it seems at first blush that if a company with positioning information released a user's information to a third party without consumer consent, the consumer would have a possible cause of action.

The intrusion upon seclusion tort is also limited, however. Suits rarely succeed if the information has been gathered in a public space.[75] Thus, as with the disclosure of personal facts tort, the fact that a person's travels to public places are observable to the public would usually defeat any claimed right of privacy in those places.[76]

### B. Privacy-Enhancing Legislation And The *U.S. West* Case

The last several years have seen a marked increase in federal legislation introduced to deal with perceived invasion of privacy problems.[77] For example, members of the 106th Congress introduced at least twenty-seven bills addressing consumer privacy or cyber-security and wiretapping.[78] However, with the notable exception of the Gramm-Leach-Bliley Act,[79] virtually none of these bills passed.[80]

In the GPS context, the most relevant piece of legislation to pass Congress in the last several years is the Telecommunications Act of 1996.[81] As explained by the Tenth Circuit Court of Appeals,[82] section

72. *See, e.g.*, Kapellas v. Kofman, 459 P.2d 912, 923 (1969) (holding that a newspaper's disclosure of the disciplinary problems of a city council candidate's teenage children did not violate the children's right of privacy).

73. RESTATEMENT (SECOND) OF TORTS § 652B.

74. *Id.* at cmt. b.

75. Singleton, *supra* note 56, at 111.

76. RESTATEMENT (SECOND) OF TORTS § 652B cmt. c (explaining that there is no liability for "observing [a person] or even taking [the person's] photograph while [the person] is walking on the public highway . . . ").

77. Singleton, *supra* note 56, at 114.

78. *See Privacy 106th Congress*, CENTER FOR DEMOCRACY & TECH. (2000), *available at* http://www.cdt.org/legislation/106th/privacy/.

79. Pub. L. No. 106-102, 113 Stat. 1338-1481 (1999) (limiting the use of financial records).

80. *Outgoing Congress Passes School, Library Internet Filtering Law*, ELECTRONIC PRIVACY LITG. REP., Jan. 8, 2001, at 10.

81. Telecomm. Act of 1996, Pub. L. No. 104-104, 110 Stat. 56, 143 (1996).

222 of the Act,[83] entitled "Privacy of customer information," states that "[e]very telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to . . . customers."[84]

The Act places restrictions on the use, disclosure of, and access to the Customer Proprietary Network Information ("CPNI") gathered by telecommunications companies.[85] CPNI includes, among other information, location, destination of calls, and amount of use of a telecommunications service.[86] The salient section of the Act with regards to CPNI is section 222(c)(1),[87] which states:

> Except as required by law or with the approval of the customer, a telecommunications carrier that receives or obtains customer proprietary network information by virtue of its provision of a telecommunications service shall only use, disclose, or permit access to individually identifiable customer proprietary network information in its provision of (A) the telecommunications service from which such information is derived, or (B) services necessary to, or used in, the provision of such telecommunications service, including the publishing of directories.[88]

The Act was amended by the Wireless Communications and Public Safety Act of 1999[89] to include location information within the definition of CPNI[90] and to explicitly require "express prior authorization" for a telecommunications provider to release location information.[91]

Though the acts taken together require customer approval before location information and other forms of CPNI are released to third parties,[92] it is not clear exactly what form customer approval must take.[93] The FCC is currently engaged in a rulemaking process, initiated at the request of the CTIA, to establish fair location information practices.[94]

---

82. U.S. West, Inc. v. Fed. Communications Comm'n, 182 F.3d 1224, 1228–29 (10th Cir. 1999).

83. 47 U.S.C. § 222 (2000).

84. *Id.* § 222(a).

85. *U.S. West*, 182 F.3d at 1228.

86. 47 U.S.C. § 222(h).

87. *Id.* § 222(c)(1).

88. *Id.*

89. Pub. L. No. 106-81, 113 Stat. 1288-1289 (1999).

90. 47 U.S.C. § 222(h)(1).

91. *Id.* § 222(f).

92. U.S. West, Inc. v. Fed. Communications Comm'n, 182 F.3d 1224, 1228–29 (10th Cir. 1999).

93. Singleton, *supra* note 56, at 115.

94. *See, e.g.*, Comments of Cingular Wireless, LLC, In the Matter of Cellular Telecommunications Industry Association's Petition for Rulemaking To Establish Fair Location Information Practices (Apr. 6, 2001), *available at* http://gullfoss2.fcc.gov/cgi-

Whatever form customer approval is required by regulation to take, such regulations will possibly face First Amendment challenge as being a violation of commercial speech. Such a First Amendment challenge was successfully raised by a telecommunications company in *U.S. West, Inc. v. Federal Communications Commission*,[95] in response to the regulations promulgated by the FCC to implement the Telecommunications Act.

Following passage of the Telecommunications Act of 1996 and before Congress amended the Act to require express customer authorization, some industry advocates argued for an "opt-out," or "implied approval" system where carriers would simply have to provide some sort of notice of their intent to use CPNI and a mechanism for customers to withdraw.[96] Consumer advocates argued for an "opt-in" approach to obtaining customer consent,[97] meaning that "a carrier would have to obtain prior express approval from a customer through written, oral, or electronic means before using the customer's CPNI."[98] The desire for an opt-in system stemmed from a concern that many consumers would not be sufficiently aware of their telecommunication company's intent to use CPNI, and so would not be vigilant enough to opt-out of the program.[99] A third approach, the most restrictive on industry, would have required carriers to obtain written consent before releasing CPNI.[100]

Because the statute was ambiguous as to how telecommunications carriers were to obtain customer approval,[101] the FCC, at the request of several telecommunications companies,[102] acted in 1998 to clarify the law by administrative order.[103] The FCC order adopted the opt-in approach, requiring customer approval through oral, written, or electronic means.[104]

A telecommunications company named U.S. West, Inc., concerned that the opt-in approach was more expensive and would result in a lower customer approval rate,[105] brought suit challenging the FCC's opt-in requirement.[106] Specifically U.S. West alleged the

bin/websql/prod/ecfs/comsrch_v2.hts.

95. 182 F.3d 1224, 1228–29 (10th Cir. 1999).

96. *U.S. West*, 182 F.3d at 1240, 1246 (Briscoe, J., dissenting).

97. *Id.* at 1240.

98. *Id.* at 1230.

99. *Id.*

100. *Id.* at 1246 (Briscoe, J., dissenting).

101. *Id.* at 1240 (Briscoe, J., dissenting) (noting that the FCC found that the statute was ambiguous in that it did not specify the type of approval required).

102. *Id.* at 1229.

103. 47 C.F.R. § 64.2007 (1998).

104. *Id.* § 64.2007(b).

105. *U.S. West*, 182 F.3d at 1240 (Briscoe, J., dissenting).

106. *Id.* at 1228.

FCC regulation infringed U.S. West's First Amendment right to engage in commercial speech.[107]

The court held that U.S. West's right to commercial speech was implicated,[108] and so applied a three-factor test from *Central Hudson Gas & Electric Corporation v. Public Service Commission of New York.*[109] In order for a regulation to be valid under *Central Hudson*: (1) the government must have a substantial state interest in regulating the speech, (2) the regulation must directly and materially advance that interest, and (3) the regulation must be no more extensive than necessary to serve the interest.[110] Applying this test, the Tenth Circuit found that the opt-in approach neither materially advanced a state interest, because the FCC only proved protecting privacy was important in the abstract;[111] nor was it narrowly tailored, because the FCC did not prove an opt-out strategy would not work.[112]

The *U.S. West* decision can be criticized on many grounds, including that U.S. West was actually objecting to Congress' law and not the FCC's interpretation of it, that the CPNI order does not really restrict speech, and that the court underestimated the importance of privacy.[113] It is not the purpose of this note, however, to offer a critique of the court's constitutional analysis. Rather, this note calls attention to the current state of privacy law with respect to location information.

If an opt-in requirement really violates the First Amendment rights of telecommunications companies, the only obvious less-restrictive option is an opt-out (i.e., implied approval) requirement. But the opt-out requirement offers very little protection to consumers who will not take the time to read the fine print at the bottom of a telecommunications contract.

Further, even if an opt-in requirements does withstand constitutional scrutiny, the Telecommunications Act offers little recourse to consumer for a violation of the Act. Though the Act creates a cause of action for violation of its terms,[114] several courts have held that a party must demonstrate damage to state a cause of action. In *Conboy v. AT&T Corp.*,[115] for example, a couple who had an unlisted telephone number brought suit after AT&T released their

107. *Id.* at 1230.
108. *Id.* at 1233.
109. 447 U.S. 557 (1980).
110. *U.S. West*, 182 F.3d at 1234 (citing *Central Hudson*, 447 U.S. at 564-65).
111. *Id.* at 1237.
112. *Id.* at 1238-39.
113. Julie Tuan, *Berkeley Technology Law Journal Annual Review of Law and Technology III*, BERKELEY TECH. L. J. 353, 360 (1998).
114. 47 U.S.C. §§ 206-207.
115. 84 F. Supp. 2d 492 (S.D.N.Y. 2000).

CPNI to an AT&T-affiliated credit-card company which was trying to collect a debt from the couple's daughter-in-law.[116] The court granted summary judgment to AT&T because the plaintiffs could not deomonstrate that they suffered any damages.[117] The court rejected the plaintiffs' contention that the monthly fee they paid to AT&T included "the privacy protections of the Telecommunications Act."[118] The fact that the plaintiffs received between thirty and fifty calls from the credit card company during a two-month span in 1998[119] also apparently did not represent a significant-enough harm to state a cause of action. Because the harm suffered as a result of an invasion of privacy is difficult to quantify in monetary terms,[120] it will be difficult for parties to state a cause of action for a provider's violation of the Act.

Finally, even if the opt-in approach seemingly required by the 1999 amendments[121] does withstand constitutional scrutiny, the Act offers no protection for people whose privacy is violated through non-cell-phone based collections of location information. The speeding rental car customer continues to have no recourse under federal legislation or through the state courts.

## III. Proposals for Ensuring the Privacy of Location Information

GPS brings with it innumerable consumer benefits. But in order for customers to freely avail themselves of those benefits, they must first trust the technology. This opinion is shared by many in the telecommunications industry. The Cellular Telecommunications Industry Association, for example, explained in their brief to the FCC that "privacy concerns regarding location information must be addressed if new services are be [sic] accepted by consumers."[122]

116. *Id.* at 497-98.

117. *Id.* at 499-500.

118. *Id.* at 499.

119. *Id.* at 497.

120. On the contrary, the loss of privacy feared by unfettered dissemination of location information is more akin to the non-monetary loss of human dignity noted by Laurence Tribe. *See* Zuckerman, *supra* note 3, text accompanying note.

121. It seems that the telecom industry does not challenge the legality or propriety of opt-in regulations in the wake of the 1999 amendments. See *supra* note 4. However, as of September, 2001, the FCC has yet to promulgate new regulations interpreting how companies are to obtain customer approval.

122. *See* Petition of the Cellular Telecommunications Industry Association for a Rulemaking to Establish Fair Location Information Practices at 4-5, In the matter of Petition for Rulemaking (Nov. 22, 2000). In a recent speech to the eBusiness Conference Expo, IBM Chairman Lou Gerstner echoed these sentiments. "What are the implications for privacy in a world where millions of people are driving Internet-enabled cars that have their movements monitored at all times? . . . [I]ndustry must send an unambiguous message that tells people: 'You can trust us.'" Lou Gerstner, Address at the eBusiness

Thus, it is imperative that either Congress or the courts act soon to ensure consumer privacy.

The First Amendment issue addressed in *U.S. West* can be raised generally as a defense to any legislation or judicially-created tort aimed at strengthening privacy rights at the expense of corporations. In this way, the *U.S. West* opinion stands as an indication of the type of obstacle that policymakers must overcome to ensure consumer privacy. This is not an insurmountable challenge.

Even the FCC's opt-in regulations would arguably pass the *Central Hudson* test if the FCC provided a more specific explanation of consumer privacy interests at stake and the regulation was narrowly tailored. Further, as Judge Briscoe explained in his dissent in *U.S. West*, some privacy legislation "arguably promotes the First Amendment rights of consumers by allowing them to call whom they wish when they wish without fear that their calling records will be disclosed to others."[123] In short, carefully crafted legislation narrowly tailored to preserve the privacy rights of consumers should withstand First Amendment scrutiny.

Another obstacle legislators will be forced to overcome is vocal industry opposition to new privacy legislation. As of March, 2001, business groups were gearing up to oppose new legislative proposals.[124] Two recently released industry-funded studies have argued that proposed restrictions on companies' ability to collect and use consumer information for marketing would dampen the national economy and trigger a 7% rise in prices for Internet and catalog purchases.[125] Meanwhile, an industry coalition including IBM, Ford, and Proctor & Gamble, planned a $30 million national advertising campaign for fall, 2001, aimed at reducing consumer fears about privacy.[126]

Industry lobbying efforts have proved successful in the past. During the 2000 state legislative sessions, industry banded together to defeat "a barrage of privacy legislation, with only very few comprehensive bills enacted."[127]

---

Conference Expo (Dec. 12, 2000).

123. U.S. West, Inc. v. Fed. Communications Comm'n, 182 F.3d 1224, 1228–29 (10th Cir. 1999).

124. Edmund Sanders, *Firms Renew Assault on Privacy Rules*, L.A. TIMES, Mar. 27, 2001, at C1.

125. *Id.* The article goes on to explain that, according to a study conducted by consumer groups, companies doing business over the Internet actually lose more than $12 billion in annual sales due to privacy concerns.

126. *Id.*

127. Owen Sweeney & James P. Toner, Jr., *Key Policy Issues; After the Gavel: Privacy in the Interim*, THE METRO. CORP. COUNSEL, Oct. 2000, at 35.

### A. A New Privacy Tort?

One bill, introduced in the California Legislature by Senator Steve Peace, contained a provision establishing a new invasion of privacy tort.[128] Though the version of the bill ultimately enacted did not contain that tort provision,[129] the provision nevertheless serves as an example of a workable solution to the location information problem. The deleted clause read:

> There shall be a cause of action for the unlawful disclosure of any personal information gathered by a commercial or government entity for a commercial or governmental purpose which that entity subsequently releases to a third party without the express permission of the person to whom the information relates. It shall be presumed in any proceeding authorized by this section that the person to whom the information released relates has sustained damages thereby.[130]

Such a bill, largely because it presumes damages, would be an excellent deterrent to prevent companies who collect location information from releasing that information without customer consent. Of course, the tort would have to be narrowly tailored and include a well-articulated state interest to be immune from the type of First Amendment argument advanced by the plaintiffs in *U.S. West.*

### B. The European Union Model

The European Union has adopted a very thorough model of privacy legislation.[131] Individuals must be informed and given the right to object before any transfer of information to a third party takes place.[132] Further, an individual must give explicit consent before a party can process personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and health or sex life.[133] This comprehensive legislation offers the consumer very specific protections and can serve as a model for American legislation.

The European directive was passed, however, at a time when the availability of location information was not an imminent problem. Any American legislation based on the European model should offer adequate protection of a customer's right to privacy in their own location information by disallowing the trading of location

128. S. 129, 1999-2000 Reg. Sess. (Cal. 1999) (as amended Aug. 26, 1999).
129. *Id.* (enacted).
130. S. 129 § 1798.100, 1999-2000 Reg. Sess. (Cal. 1999) (as amended Aug. 26, 1999).
131. Council Directive 95/46/EC, 1995 O.J. (L 281).
132. *Id.* at Art. 14(b).
133. *Id.* at Art. 8(1)-(2).

information absent explicit customer permission and creating a cause of action with a presumption of damages.

## Conclusion

From reduced car insurance, to increased personal security, to real-time, location-based personal services, GPS stands poised to ease our daily lives. In order for GPS to achieve its potential, however, legislators, courts, businesses, and the public at large must first deal with some very real privacy issues. After all, only if the public trusts a technology can they truly come to rely on it.

Under the current state of privacy law, the public cannot be expected to trust businesses who collect location information. Thus, legislators and courts must act now to establish a legal framework for protection of personal location information. State legislative proposals and a European Union directive offer some promising legal options – it is now up to Congress, state legislatures, and the courts to see to it that those options are explored.

***